ELSEVIER

Available online at www.sciencedirect.com
SCIENCE DIRECT®

Journal of Algebra 268 (2003) 700–722

JOURNAL OF Algebra

www.elsevier.com/locate/jalgebra

Separable exterior squares over finite fields

Duncan Brydon

Mathematical Institute, University of Oxford, 24–29 St. Giles, Oxford, OX1 3LB, UK

Received 29 October 2002

Communicated by Jan Saxl

Abstract

The paper concerns exterior squares of polynomials and matrices over the finite field $\mathbb{F}_q$ for large q. We find the probability that monic $f \in \mathbb{F}_q[t]$ has a non-separable exterior square. We then find the probability that $X \in \mathrm{GL}(d,q)$ has an exterior square which is non-separable, non-cyclic or non-semisimple. This should have applications in recognising $\mathrm{GL}(V)$ in its action on $V \wedge V$, when V is a d-dimensional vector space over $\mathbb{F}_q$.

1. Introduction

Let f be a monic polynomial of degree d over a field F with roots $\lambda_1, \ldots, \lambda_d$ in its splitting field over F. Then the *exterior square of* f is denoted by $f^{\wedge 2}$ and defined by

$$f^{\wedge 2}(t) = \prod_{1 \leqslant i < j \leqslant d} (t - \lambda_i \lambda_j).$$

A polynomial $f \in \mathbb{F}_q[t]$ is said to be *separable* if it has no repeated roots in its splitting field.

The matrix representing the action of a given matrix X on the exterior square of the underlying vector space, with respect to a standard basis, is called the *exterior square of* X and we denote it by $X^{\wedge 2}$. We shall denote the minimal and characteristic polynomials of a matrix $X \in \mathrm{GL}(d,q)$ by m_X and c_X, respectively. A matrix X is said to be *separable* if c_X is separable and is said to be *semisimple* if m_X is separable. We say that $X \in \mathrm{GL}(d,q)$ is cyclic if $\mathrm{c}_X = \mathrm{m}_X$.

E-mail address: brydon@maths.ox.ac.uk.

0021-8693/$ – see front matter
doi:10.1016/S0021-8693(03)00272-2

Definition 1. Define $p_{\mathrm{ns}}(d,q)$ to be the probability that $f \in \mathbb{F}_q[t]$ has a non-separable exterior square. Define $P_{\mathrm{ns}}(d,q)$ to be the probability that $X \in \mathrm{GL}(d,q)$ has a non-separable exterior square, $P_{\mathrm{nc}}(d,q)$ to be the probability that $X \in \mathrm{GL}(d,q)$ has a non-cyclic exterior square and $P_{\mathrm{nss}}(d,q)$ to be the probability that $X \in \mathrm{GL}(d,q)$ has a non-semisimple exterior square.

In this paper, we prove the following theorems.

Theorem 2. *For $d \geqslant 2$, $p_{\mathrm{ns}}(d,q) = 2q^{-1} + O(q^{-2})$.*

Theorem 3. *For $d \geqslant 3$,*

$$P_{\mathrm{ns}}(d,q) = 2q^{-1} + O\big(q^{-2}\big), \qquad P_{\mathrm{nc}}(d,q) = q^{-1} + O\big(q^{-2}\big),$$
$$P_{\mathrm{nss}}(d,q) = q^{-1} + O\big(q^{-2}\big).$$

The latter theorem should be useful in designing algorithms to recognise $\mathrm{GL}(V)$ in its action on $V \wedge V$. In [1], the author finds $P_{\mathrm{ns}}(4,q)$, $P_{\mathrm{nc}}(4,q)$ and $P_{\mathrm{nss}}(4,q)$ exactly. The interested reader might also refer to the work of Catherine Greenhill [3,4] in which first steps are taken towards developing an algorithm for the extraction of exterior square roots of matrices.

2. Preliminaries

The following lemmas are well known and their proofs are omitted. For details, we refer the reader to [1].

Lemma 4. *Let $\rho : \mathrm{GL}(d,F) \to \mathrm{GL}\big(\binom{d}{2}, F\big)$ be defined by $\rho : X \mapsto X^{\wedge 2}$. Then ρ is a homomorphism and*

$$\ker\rho = \begin{cases} \{\pm I\} & \text{if } d > 2, \\ \mathrm{SL}(2,F) & \text{if } d = 2. \end{cases}$$

Lemma 5. *Let $X \in \mathrm{M}(d,F)$. Then $\mathrm{c}_{X^{\wedge 2}}(t) = \mathrm{c}_X^{\wedge 2}(t)$.*

Definition 6. The exterior square of $\mathrm{GL}(d,F)$ is denoted by $\bigwedge^2 \mathrm{GL}(d,F)$ and defined by

$$\bigwedge^2 \mathrm{GL}(d,F) = \big\{ X^{\wedge 2} \bigm| X \in \mathrm{GL}(d,F) \big\}.$$

From Lemma 4, we see that $\bigwedge^2 \mathrm{GL}(d,F)$ is a group. We now wish to determine if a similar statement to that in Lemma 5 can be made regarding $\mathrm{m}_{X^{\wedge 2}}$ and $\mathrm{m}_X^{\wedge 2}$. Let us make the following definition.

Definition 7. Let $n \in \mathbb{N}$ and λ be an element of the field F. Then $J_n(\lambda)$ denotes the $n \times n$ Jordan block with associated eigenvalue λ. That is,

$$J_n(\lambda) := \begin{pmatrix} \lambda & 1 & & & 0 \\ & \lambda & 1 & & \\ & & \ddots & \ddots & \\ & & & \ddots & 1 \\ 0 & & & & \lambda \end{pmatrix}.$$

Now we shall state and prove our theorem about $\mathrm{m}_X^{\wedge 2}$ and $\mathrm{m}_{X^{\wedge 2}}$. For a matrix $X \in \mathrm{GL}(d, F)$ we denote by F_X the splitting field of c_X over F.

Theorem 8. *Let $X \in \mathrm{GL}(d, F)$ where F need not be finite. Over F_X, let X have Jordan canonical form $J_1 \oplus J_2 \oplus \cdots \oplus J_k$ where*

$$J_i = J_{n_{i,1}}(\lambda_i) \oplus J_{n_{i,2}}(\lambda_i) \oplus \cdots \oplus J_{n_{i,s_i}}(\lambda_i) \quad \text{with } n_{i,1} \geqslant n_{i,2} \geqslant \cdots \geqslant n_{i,s_i}.$$

Then $\mathrm{m}_{X^{\wedge 2}}$ divides $\mathrm{m}_X^{\wedge 2}$ provided there does not exist i such that $(n_{i,1}, n_{i,2}) \in \{(2,1), (3,2), (2,2), (3,3), (4,4)\}$.

We shall need the following lemma whose proof is routine. With the notation of Theorem 8.

Lemma 9. *$J_{n_i}(\lambda_i) \otimes J_{n_j}(\lambda_j)$ has minimal polynomial dividing $(t - \lambda_i\lambda_j)^{n_i+n_j-1}$ and $J_i \otimes J_j$ has minimal polynomial dividing $(t - \lambda_i\lambda_j)^{n_{i,1}+n_{j,1}-1}$.*

Proof of Theorem 8. Let α be the linear map represented by the matrix X with respect to the standard basis. Regarding V as an $F[t]$-module via α, we write $V_n(\lambda)$ for a cyclic submodule of V of order $(t-\lambda)^n$. Now let us write $V = \bigoplus_i W_i$ where $W_i = \bigoplus_j V_{n_{i,j}}(\lambda_i)$ so that

$$X|_{W_i} = J_i \quad \text{and} \quad X|_{V_{n_{i,j}}(\lambda_i)} = J_{n_{i,j}}(\lambda_i).$$

For all i, let $m_i := n_{i,1}$. Then $\mathrm{m}_X(t) = \prod_i (t-\lambda_i)^{m_i}$ and so

$$\mathrm{m}_X^{\wedge 2}(t) = \prod_i \left(t - \lambda_i^2\right)^{\binom{m_i}{2}} \times \prod_{i<j} (t - \lambda_i\lambda_j)^{m_i m_j}. \tag{1}$$

Also we have

$$V \wedge V = \left(\bigoplus_i W_i \wedge W_i\right) \oplus \left(\bigoplus_{i<j} W_i \otimes W_j\right). \tag{2}$$

The condition $\mathrm{m}_{X^{\wedge 2}} \mid \mathrm{m}_X^{\wedge 2}$ is equivalent to $\mathrm{m}_X^{\wedge 2}(X^{\wedge 2}) = 0$. Clearly $\mathrm{m}_X^{\wedge 2}(X^{\wedge 2})$ annihilates $V \wedge V$ if and only if it annihilates each of the summands in (2). From (1), we have

$$\mathrm{m}_X^{\wedge 2}\big(X^{\wedge 2}\big) = \prod_i \big(X^{\wedge 2} - \lambda_i^2 I\big)^{\binom{m_i}{2}} \times \prod_{i<j} \big(X^{\wedge 2} - \lambda_i \lambda_j I\big)^{m_i m_j}.$$

It follows from Lemma 9 that the minimum polynomial of $W_i \otimes W_j$ divides $(t - \lambda_i \lambda_j)^{m_i + m_j - 1}$ and $m_i + m_j - 1 \leqslant m_i m_j$ with equality if and only if one of m_i or m_j is 1. Hence the factor $(X^{\wedge 2} - \lambda_i \lambda_j I)^{m_i m_j}$ of $\mathrm{m}_X^{\wedge 2}(X^{\wedge 2})$ kills $W_i \otimes W_j$.

We now need only concern ourselves with the summands $W_i \wedge W_i$. Note that we may assume that $m_i > 1$. We have

$$W_i \wedge W_i = \left(\bigoplus_j V_{n_{i,j}}(\lambda_i) \wedge V_{n_{i,j}}(\lambda_i) \right) \oplus \left(\bigoplus_{j<k} \big(V_{n_{i,j}}(\lambda_i) \otimes V_{n_{i,k}}(\lambda_i) \big) \right).$$

The dimension of $V_{n_{i,j}}(\lambda_i) \wedge V_{n_{i,j}}(\lambda_i)$ is $\binom{n_{i,j}}{2}$ which is at most $\binom{m_i}{2}$ and so the factor $(X^{\wedge 2} - \lambda_i \lambda_j I)^{\binom{m_i}{2}}$ of $\mathrm{m}_X^{\wedge 2}(X^{\wedge 2})$ kills $V_{n_{i,j}}(\lambda_i) \wedge V_{n_{i,j}}(\lambda_i)$.

So now we need only concern ourselves with the summands

$$V_{n_{i,j}}(\lambda_i) \otimes V_{n_{i,k}}(\lambda_i).$$

From Lemma 9 , we have that the minimal polynomial of $J_{n_{i,j}}(\lambda_i) \otimes J_{n_{i,k}}(\lambda_i)$ divides $(t - \lambda_i^2)^{n_{i,j} + n_{i,k} - 1}$ and $n_{i,j} + n_{i,k} - 1 \leqslant m_i + n_{i,2} - 1$. It follows that $\mathrm{m}_X^{\wedge 2}(X^{\wedge 2}) \neq 0$ only if there exists i such that

$$m_i + n_{i,2} - 1 > \frac{1}{2} m_i (m_i - 1).$$

This implies that

$$-\frac{\sqrt{17}}{2} < m_i - \frac{5}{2} < \frac{\sqrt{17}}{2},$$

but because m_i is a positive integer, we need $1 \leqslant m_i < 5$.

One now checks easily that $\mathrm{m}_X^{\wedge 2}(X^{\wedge 2})$ is non-zero only if

$$(n_{i,1}, n_{i,2}) \in \big\{ (2,1), (3,2), (2,2), (3,3), (4,4) \big\}. \qquad \square$$

Theorem 10. *For $d \geqslant 3$, if $X \in \mathrm{GL}(d, F)$ is non-separable then $X^{\wedge 2}$ is non-separable.*

Proof. If X is non-separable then $\mathrm{c}_X(t) = (t - \lambda)^2 f(t)$ for some $\lambda \in F_X$. Since $\deg \mathrm{c}_X(t) \geqslant 3$, we have $\deg f(t) \geqslant 1$. Let μ be a root of $f(t)$ in F_X. Then $(t - \lambda\mu)^2$ will be a factor of $\mathrm{c}_{X^{\wedge 2}}(t)$ over F_X. $\square$

Theorem 11. *For $d \geqslant 3$, if $X \in \mathrm{GL}(d, F)$ is non-cyclic then $X^{\wedge 2}$ is non-cyclic.*

Proof. Suppose firstly that the assumptions of Theorem 8 hold so that $\mathrm{m}_{X^{\wedge 2}} \mid \mathrm{m}_X^{\wedge 2}$. If $X^{\wedge 2}$ is cyclic, then $\mathrm{m}_{X^{\wedge 2}} = \mathrm{c}_{X^{\wedge 2}} = \mathrm{c}_X^{\wedge 2}$. Together, these statements imply that $\mathrm{c}_X^{\wedge 2} \mid \mathrm{m}_X^{\wedge 2}$ and so $\mathrm{m}_X = \mathrm{c}_X$; in other words, X is cyclic. Hence, under the assumptions of Theorem 8, if X is non-cyclic then $X^{\wedge 2}$ is non-cyclic too.

Now suppose that the assumptions of Theorem 8 do not hold and that X is non-cyclic. Let us write X in Jordan canonical form over the splitting field of m_X, so we have

$$X = \bigoplus_i J_{n_i}(\lambda_i). \tag{3}$$

It follows that $X^{\wedge 2}$ can be written in the form

$$X^{\wedge 2} = \bigoplus_i \big(J_{n_i}(\lambda_i)\big)^{\wedge 2} \oplus \bigoplus_{i<j} \big(J_{n_i}(\lambda_i) \otimes J_{n_j}(\lambda_j)\big). \tag{4}$$

If X has a summand

$$J_l(\lambda) \oplus J_m(\lambda) \oplus J_n(\mu) \tag{5}$$

then $X^{\wedge 2}$ will have a summand

$$\big(J_l(\lambda) \otimes J_n(\mu)\big) \oplus \big(J_m(\lambda) \otimes J_n(\mu)\big). \tag{6}$$

By Lemma 9, the matrix in (6) has minimal polynomial dividing $(t - \mu\lambda)^{n+\max(l,m)-1}$, but characteristic polynomial $(t - \mu\lambda)^{n(l+m)}$, and so is not cyclic. Hence $X^{\wedge 2}$ is not cyclic.

If X does not have a summand of the form (5), then X must have Jordan canonical form $J_{n_1}(\lambda) \oplus J_{n_2}(\lambda)$ and the possible choices for (n_1, n_2) are given by Theorem 8. It is straightforward to check that each of these makes $X^{\wedge 2}$ non-cyclic. □

The following lemma is well known.

Lemma 12. *Suppose that $X \in \mathrm{GL}(d, F)$ where $d \geqslant 3$, $\mathrm{char}\, F = p < \infty$, and $\mathrm{ord}(X) = n$. Then X is semisimple if and only if $p \nmid n$.*

Theorem 13. *Let X belong to $\mathrm{GL}(d, q)$ where $d \geqslant 3$. Then X is semisimple if and only if $X^{\wedge 2}$ is semisimple.*

Proof. Suppose $d \geqslant 3$ and let $\rho : \mathrm{GL}(d, q) \to \bigwedge^2 \mathrm{GL}(d, q)$ be defined by $\rho : X \mapsto X^{\wedge 2}$. If $\mathrm{char}\, F = 2$ then ρ is a monomorphism (by Lemma 4) and so $\mathrm{ord}(X^{\wedge 2}) = \mathrm{ord}(X)$. If $\mathrm{char}\, F > 2$ then $\ker \rho = \{\pm I\}$ (again by Lemma 4) and so $\mathrm{ord}(X^{\wedge 2})$ equals $\mathrm{ord}(X)$ or $\frac{1}{2}\,\mathrm{ord}(X)$. In either case, if $\mathrm{char}\, F = p$ then

$$p \nmid \mathrm{ord}(X) \quad \Leftrightarrow \quad p \nmid \mathrm{ord}\big(X^{\wedge 2}\big). \tag{7}$$

But Lemma 12 tells us that

$$X \text{ is semisimple} \quad \Leftrightarrow \quad p \nmid \operatorname{ord}(X). \tag{8}$$

The result now follows from (7) and (8). □

Note that Theorem 13 holds with $\mathrm{GL}(d, q)$ replaced by $\mathrm{GL}(d, F)$ for any field F. This is proved in [1], for example, but will not be required here.

3. Exterior squares of polynomials

In this section, we shall prove Theorem 2. In [1], with certain refinements to the arguments presented here, the author obtains the result

$$p_{\mathrm{ns}}(d, q) = 2q^{-1} + \epsilon(q),$$

where $\epsilon(q) \leqslant 1050q^{-2}$ for $q \geqslant 5$. Since the constant 1050 is far from optimal, and for reasons of brevity, we shall not attempt to keep track of the constants implicit in the big 'Oh' notation in this paper.

We begin with some definitions. Let $\mathbb{F}_{q^i}^{-}$ denote the set of all elements of the field $\mathbb{F}_{q^i}$ which belong to no proper subfield of $\mathbb{F}_{q^i}$. We shall call a polynomial $f \in \mathbb{F}_q[t]$ nearly separable if $f(t) = g(t)(t-\lambda)^2$ where g is separable and $g(\lambda) \neq 0$.

Define $p_{\mathrm{sns}}(d, q)$ to be the probability that a polynomial $f \in \mathbb{F}_q[t]$ is separable and has a non-separable exterior square. It is clear that the exterior square of any non-separable polynomial of degree at least 3 is non-separable (the proof is the same as that of Theorem 10). From [5], we have that the probability of a monic polynomial in $\mathbb{F}_q[t]$ of degree $d > 1$ being non-separable is q^{-1}. Hence

Lemma 14. *For $d \geqslant 3$, $p_{\mathrm{ns}}(d, q) = p_{\mathrm{sns}}(d, q) + q^{-1}$.*

To prove Theorem 2, it now remains only to find $p_{\mathrm{sns}}(d, q)$. We shall require the following identity which is clear.

Lemma 15. *For $a, b, n \in \mathbb{N}$,*

$$\left\lfloor \frac{a}{b} n \right\rfloor + \left\lceil \frac{b-a}{b} n \right\rceil = n.$$

We now describe an argument which we shall use frequently in the rest of this section.

Lemma 16 (The index cycling argument). *Suppose an irreducible polynomial f of degree n in $\mathbb{F}_q[t]$ has roots $\alpha, \alpha^{q^i}, \alpha^{q^j}$, and α^{q^k} such that $\alpha\alpha^{q^i} = \alpha^{q^j}\alpha^{q^k}$. Then there exist $u, v, w \leqslant \lfloor 3n/4 \rfloor$ such that all roots β of f satisfy $\beta^{1+q^u} = \beta^{q^v+q^w}$. Furthermore, if $\{u, v, w\} = \{x, y, z\}$ where $0 < x < y < z < n$, then $\max\{x, y-x, z-y, n-z\} = n-z$.*

In what follows we shall refer to the quantities x, $y-x$, $z-y$, and $n-z$ as gaps. Lemma 16 tells us that, without loss of generality, we may assume that the maximum gap comes at the end, that is, equals $n-z$.

Proof of Lemma 16. Define $\{a,b,c\}$ to be the set $\{i,j,k\}$ relabelled so that $0<a<b<c<n$. Now suppose that $[s,t]$ is the interval of maximum length (or an interval of maximal length) in the set $\{[0,a],[a,b],[b,c],[c,n]\}$. Clearly $t-s\geqslant\lceil n/4\rceil$ and therefore

$$n-(t-s)\leqslant\lfloor 3n/4\rfloor. \tag{9}$$

Define $\alpha_1:=\alpha^{q^t}$. Then the set $\{\alpha,\alpha^{q^i},\alpha^{q^j},\alpha^{q^k}\}$ is equal to the set

$$\left\{\alpha_1^{q^{n-t}},\alpha_1^{q^{n-t+i}},\alpha_1^{q^{n-t+j}},\alpha_1^{n-t+k}\right\}=\left\{\alpha_1,\alpha_1^{q^x},\alpha_1^{q^y},\alpha_1^{q^z}\right\}$$

for positive integers $x<y<z<n$. Furthermore, we see that α^{q^s} must equal $\alpha_1^{q^z}$. Therefore $n-z=\max\{x,y-x,z-y,n-z\}$ and $z=n-(t-s)$ which we know from Eq. (9) is not more than $\lfloor 3n/4\rfloor$. It follows that $x,y,z\leqslant\lfloor 3n/4\rfloor$. Hence

$$\alpha_1^{1+q^u}=\alpha_1^{q^v+q^w} \tag{10}$$

for some $u,v,w\leqslant\lfloor 3n/4\rfloor$. (Specifically $\{u,v,w\}=\{x,y,z\}$.)

For any integer l, raising both sides of (10) to the power q^l gives

$$\left(\alpha_1^{q^l}\right)^{1+q^u}=\left(\alpha_1^{q^l}\right)^{q^v+q^w}.$$

Hence all roots β of f satisfy $\beta^{1+q^u}=\beta^{q^v+q^w}$ and, as we have seen, $u,v,w\leqslant\lfloor 3n/4\rfloor$. □

Similar arguments yield the following three lemmas.

Lemma 17. *Let g be an irreducible polynomial over $\mathbb{F}_q$. Let f be an irreducible polynomial of degree n over $\mathbb{F}_q$ distinct from g and having a root α satisfying $\alpha^{1+q^i-q^j}=\beta$ for some root β of g and for some i and j. Then there exist $u,v\leqslant\lfloor 2n/3\rfloor$ such that for every root γ of f, there is a root δ of g such that either $\gamma^{1+q^u-q^v}=\delta$ or $\gamma^{q^u+q^v-1}=\delta$.*

Lemma 18. *Let h_1 and h_2 be irreducible polynomials in $\mathbb{F}_q[t]$ with degrees n_1 and n_2, respectively.*

If h_1 and h_2 have roots α_1 and α_2, respectively, satisfying $\alpha_1^{1+q^i}=\alpha_2^{1+q^j}$ for some integers i and j, then there exist roots β_1 and β_2 of h_1 and h_2, respectively, and integers $k\leqslant\lfloor n_1/2\rfloor$ and $l\leqslant\lfloor n_2/2\rfloor$ such that $\beta_1^{1+q^k}=\beta_2^{1+q^l}$.

If h_1 and h_2 have roots α_1 and α_2, respectively, satisfying $\alpha_1^{q^i-1}=\alpha_2^{q^j-1}$ for some integers i and j, then there exist roots β_1 and β_2 of h_1 and h_2, respectively, and integers $k\leqslant\lfloor n_1/2\rfloor$ and $l\leqslant\lfloor n_2/2\rfloor$ such that either $\beta_1^{q^k-1}=\beta_2^{q^l-1}$ or $\beta_1^{q^k-1}=\beta_2^{1-q^l}$.

Lemma 19. *Let h_1, h_2, and f be irreducible polynomials in $\mathbb{F}_q[t]$ and let f have degree n.*

If f has a root α satisfying $\alpha^{1+q^i} = \beta_1\beta_2$ for some roots β_1 and β_2 of h_1 and h_2, respectively, and for some i, then there exists $j \leqslant \lfloor n/2 \rfloor$ such that for all roots δ of f, there are roots γ_1 of h_1 and γ_2 of h_2 such that $\delta^{1+q^j} = \gamma_1\gamma_2$.

If f has a root α satisfying $\alpha^{q^i-1} = \beta_1\beta_2^{-1}$ for some roots β_1 and β_2 of h_1 and h_2, respectively, and for some i, then there exists $j \leqslant \lfloor n/2 \rfloor$ such that for all roots δ of f, there are roots γ_1 of h_1 and γ_2 of h_2 such that either $\delta^{q^j-1} = \gamma_1\gamma_2^{-1}$ or $\delta^{q^j-1} = \gamma_1^{-1}\gamma_2$.

Lemma 20. *The number N_4 of monic irreducible quartic polynomials in $\mathbb{F}_q[t]$ with a root α satisfying $\alpha\alpha^{q^i} = \alpha^{q^j}\alpha^{q^k}$ for some non-zero distinct i, j, and k is $\frac{1}{4}q(q^2-1)$ if q is odd and $\frac{1}{4}q^2(q-1)$ if q is even.*

Proof. For $n \mid q^r - 1$, define $C_{q^r}(n)$ to be the cyclic subgroup of $\mathbb{F}_{q^r}^*$ of order n. It is straightforward to show that any suitable α must belong to

$$S = \big(C_{q^4}\big((q^2+1)(q-1)\big) \cup C_{q^4}\big(\mu\big(q^2-1\big)\big)\big)\big\backslash\big(C_{q^4}\big(q^2-1\big)\big).$$

The result follows by noting that if one root of f satisfies $\alpha^{1+q^i} = \alpha^{q^j+q^k}$ for particular i, j, and k, then so do all its conjugates. Hence N_4 is $|S|/4$. □

We shall now show that $p_{\mathrm{sns}}(d,q) = q^{-1} + O(q^{-2})$. Applying Lemma 14, it will follow that $p_{\mathrm{ns}} = 2q^{-1} + O(q^{-2})$, as required. We will denote the degree of a polynomial f by ∂f.

Theorem 21. *For $d \geqslant 3$, $p_{\mathrm{sns}}(d,q) = q^{-1} + O(q^{-2})$.*

Proof. Suppose that $f \in \mathbb{F}_q[t]$ is monic and separable of degree d and has $f^{\wedge 2}$ non-separable. Then there exist roots $\alpha_1, \alpha_2, \alpha_3$, and α_4 of f such that $\alpha_1\alpha_2 = \alpha_3\alpha_4$.

There are five cases to consider.

Case 1: All the α_i are roots of the same irreducible factor of f.
Case 2: The α_i are roots of distinct irreducible factors of f.
Case 3: The roots split into two pairs, one pair being roots of one irreducible factor of f, the other roots of another.
Case 4: Exactly two of the α_i are roots of the same irreducible factor of f.
Case 5: Exactly three of the α_i are roots of the same irreducible factor of f.

Throughout this proof, we will assume $q \geqslant 5$. This is sensible because a contribution of $\frac{1}{8}q^{-1} + O(q^{-2})$ comes from those polynomials of Case 2 having four linear factors which are distinct and distinct from t. The minimal polynomial of α_i will be denoted by h_i and the degree of h_i by n_i. We shall denote by $[z^i]g(z)$ the coefficient of z^i in the Maclaurin expansion of $g(z)$.

We will give the arguments used to deal with Cases 1, 2, and 5. The arguments used for the other cases are similar and can be found in [1]. For Cases 3 and 4, we make use of

Lemmas 18 and 19, respectively. We find that the probabilities of Cases 3 and 4 occurring modulo $O(q^{-2})$ are $\frac{3}{8}q^{-1}$ and $\frac{1}{4}q^{-1}$, respectively.

Case 1. Suppose h_1 is an irreducible polynomial of degree n_1 with roots $\alpha, \alpha^{q^i}, \alpha^{q^j}$, and α^{q^k} satisfying

$$\alpha\alpha^{q^i} = \alpha^{q^j}\alpha^{q^k}. \tag{11}$$

Case 1.1 ($n_1 = 4$). To construct a polynomial of Case 1.1, we first choose h_1 for which there are N_4 choices. From Lemma 20 we have that

$$N_4 = \begin{cases} \frac{1}{4}q(q^2-1) & \text{if } q \text{ is odd,} \\ \frac{1}{4}q^2(q-1) & \text{if } q \text{ is even.} \end{cases}$$

Then we choose a separable polynomial h of degree $d-4$ such that $h_1 \nmid h$. The number of choices for h is

$$q^{d-4}\left[z^{d-4}\right]\left(1+\left(\frac{z}{q}\right)^4\right)^{-1}\left(1+z+\left(1-q^{-1}\right)\sum_{i=2}^{\infty} z^i\right)$$

which equals $q^{d-4}(1-q^{-1}+O(q^{-2}))$ if $d \geqslant 6$ and q if $d = 5$. This follows from the fact that

$$1+z+\left(1-q^{-1}\right)\sum_{i=2}^{\infty} z^i$$

is the generating function for separable polynomials. Hence the probability of this case occurring is $\frac{1}{4}q^{-1}+O(q^{-2})$.

Case 1.2 ($n_1 \geqslant 5$). From the index cycling argument, it follows that $\exists u, v, w \leqslant \lfloor 3n_1/4 \rfloor$ such that all roots β of h_1 satisfy $\beta^{1+q^u} = \beta^{q^v+q^w}$. Define $r_n := \lfloor 3n/4 \rfloor$. First note that there are $3\binom{r_{n_1}}{3}$ equations of the form

$$x^{1+q^u} = x^{q^v+q^w} \quad \text{with } u, v, w \leqslant r_{n_1}. \tag{12}$$

Once n_1, u, v, and w are chosen, (12) gives a polynomial equation of degree $\max\{1+q^u, q^v+q^w\} \leqslant 2q^{\lfloor 3n_1/4 \rfloor}$ which α must satisfy, so there are at most $2q^{\lfloor 3n_1/4 \rfloor}$ possibilities for α once n_1, u, v, and w are fixed. So the number of irreducible polynomials of degree n_1 that we are looking for is at most $2n_1^3 q^{\lfloor 3n_1/4 \rfloor}$.

To construct a separable polynomial f of Case 1.2, we choose an irreducible polynomial h_1 of degree n_1 with a root satisfying (11) and then a separable polynomial h of degree $d-n_1$ such that $h_1 \nmid h$. Then we define $f := h_1 h$. There are less than q^{d-n_1} choices for h. Hence the probability of Case 1.2 occurring is less than

$$2\left(\left(5^3+6^3+7^3\right)q^{-2}+\sum_{n_1=8}^{\infty}n^3q^{-n_1/4}\right)=O\left(q^{-2}\right).$$

Case 2. A polynomial f of Case 2 has irreducible factors h_1, h_2, h_3, and h_4 with roots $\alpha_1, \alpha_2, \alpha_3$, and α_4, respectively, such that

$$\alpha_1\alpha_2=\alpha_3\alpha_4. \tag{13}$$

Without loss of generality, assume that $n_1 \geqslant n_i$ for $i \in \{2,3,4\}$. Suppose that $n_1 \geqslant 2$. There are at most $n_2n_3n_4 \leqslant n_1^3$ choices for α_2, α_3, and α_4. But then α_1 and hence h_1 is determined by (13). There are at most n_1^3 choices for n_2, n_3, and n_4 once n_1 is chosen. And so the proportion of polynomials covered by this case is at most $\sum_{n_1\geqslant 2} n_1^6q^{-n_1}=O(q^{-2})$. So the only situation left to consider is when $n_i=1$ for all i. Let us do so now.

Define

$$N:=\left\{(\alpha_1,\alpha_2,\alpha_3,\alpha_4)\in(F^*)^4 \;\middle|\; \alpha_1,\alpha_2,\alpha_3,\alpha_4 \text{ are distinct but } \alpha_1\alpha_2,\alpha_1\alpha_3,\alpha_1\alpha_4,\alpha_2\alpha_3,\ \alpha_2\alpha_4,\alpha_3\alpha_4 \text{ are not distinct}\right\}.$$

Let $\{i,j,k,l\}=\{1,2,3,4\}$ and define

$$N_{ij|kl}=\left\{(a_1,a_2,a_3,a_4)\in(F^*)^4 \;\middle|\; a_1,a_2,a_3,a_4 \text{ are distinct and } a_ia_j=a_ka_l\right\}.$$

Then

$$N=N_{12|34}\cup N_{13|24}\cup N_{14|23}$$

because the only equalities possible amongst $a_1a_2, a_1a_3, a_1a_4, a_2a_3, a_2a_4$, and a_3a_4 consistent with the condition that a_1, a_2, a_3, and a_4 should be distinct are

$$a_1a_2=a_3a_4, \tag{14}$$

$$a_1a_3=a_2a_4, \tag{15}$$

$$a_1a_4=a_2a_3. \tag{16}$$

Let us calculate the size of $N_{12|34}$ which, by symmetry, will also be the size of $N_{13|24}$ and $N_{14|23}$. We have

$$(q-1)(q-2)(q-5)\leqslant\left|N_{12|34}(q-1)(q-2)(q-3)\right|.$$

The upper bound arises from the fact that α_4 is determined by (14) once α_1, α_2, and α_3 are chosen. To see how the lower bound comes about, note that a choice of α_1, α_2, and α_3 can always be extended to a valid element of A, provided that α_1, α_2, and α_3 are distinct, and $\alpha_3^2\neq\alpha_1\alpha_2$. Hence we have $(q-1)(q-2)$ choices for α_1 and α_2 and then at least $(q-1)-4$ choices for α_3. This argument shows that $|N_{12|34}|=q^3+O(q^2)$.

Also, we have that $|N_{12|34} \cap N_{13|24}| = O(q^2)$. This is because any element in both $N_{12|34}$ and $N_{13|24}$ must satisfy $\alpha_2 = \pm\alpha_3$ as well as satisfying (14), and so is determined once α_1, α_2 and a sign is chosen. A similar argument holds for $|N_{12|34} \cap N_{14|23}|$, $|N_{13|24} \cap N_{14|23}|$, and $|N_{12|34} \cap N_{13|24}| \cap N_{14|23}|$. Combining these bounds gives us that $|N| = 3q^3 + O(q^2)$. This is the number of ordered quadruples, so the number of unordered quadruples is $|N|/24$. This is the number of products $h_1h_2h_3h_4$ of distinct linear factors such that the exterior square of $h_1h_2h_3h_4$ is non-separable. To construct a polynomial f of Case 2 with all the n_i equal to 1, we choose such a product and then choose a separable polynomial g of degree $d-4$ such that none of the h_i are factors of g. There are $q-4$ choices for a linear g. For $d \geqslant 2$, there are $q^{d-4}(1 - 5q^{-1} + O(q^{-2}))$ choices for g. It follows that the probability of Case 2 occurring is $\frac{1}{8}q^{-1} + O(q^{-2})$.

Case 5. Suppose f is a separable polynomial of Case 5. Then f has irreducible factors h_1 and h_2 with roots α_1 and α_2, respectively, satisfying $\alpha_1^{1+q^i} = \alpha_1^{q^j}\alpha_2$ for some i and j. Let n_1 and n_2 be the degrees of h_1 and h_2, respectively. Note that n_2 divides n_1.

From Lemma 17, there exist $r, s \leqslant \lfloor 2n_1/3 \rfloor$ such that all roots β_1 of h_1 satisfy one of

$$\beta_1^{1+q^r} = \beta_1^{q^s}\beta_2, \tag{17}$$

$$\beta_1^{q^r+q^s} = \beta_1\beta_2 \tag{18}$$

for some root β_2 of h_2.

Let us count the number of pairs (β_1, β_2) satisfying (17) once n_1 is fixed. We have q^{n_2} choices for β_2 and at most n_1^2 choices for r and s. Then (17) is a polynomial equation of degree at $\max\{1+q^r, q^s\} \leqslant 2q^{\lfloor 2n_1/3 \rfloor}$ that β_1 must satisfy. Since n_2 divides n_1, there are at most n_1 choices for n_2 once n_1 is chosen. Hence the number of pairs (β_1, β_2) satisfying (17) once n_1 is chosen is at most $n_1^3 q^{\lfloor 2n_1/3 \rfloor}$. A similar argument shows that the number of pairs (β_1, β_2) satisfying (18) for fixed n_1 is also at most $n_1^3 q^{\lfloor 2n_1/3 \rfloor}$. It follows that the proportion of polynomials in Case 5 is at most

$$\sum_{n_1 \geqslant 4} n_1^3 q^{\lfloor 2n_1/3 \rfloor - n_1} = O\big(q^{-2}\big).$$

We have now dealt with all five cases. Define p_i to be the probability of a polynomial of case i occurring. Then we have shown that

$$\sum_{i=1}^{5} p_i = q^{-1} + O\big(q^{-2}\big). \tag{19}$$

Note that the contribution to the coefficient of q^{-1} in (19) comes from the probability that f falls into one of the following four sets:

$$E_1(d) = \big\{ f \in \mathbb{F}_q[t] \;\big|\; \partial f = d,\ f \text{ is monic, separable with an irreducible quartic factor } h_1 \text{ with a root } \alpha \text{ satisfying } \alpha\alpha^{q^i} = \alpha^{q^j}\alpha^{q^k} \text{ for some } i, j, k \big\},$$

$$E_2(d) = \{ f \in \mathbb{F}_q[t] \mid \partial f = d,\ f \text{ is separable and has four linear factors } h_1, h_2, h_3, \text{ and } h_4 \text{ with roots } \alpha_1, \alpha_2, \alpha_3, \text{ and } \alpha_4, \text{ respectively, satisfying } \alpha_1\alpha_2 = \alpha_3\alpha_4 \},$$

$$E_3(d) = \{ f \in \mathbb{F}_q[t] \mid \partial f = d,\ f \text{ is monic, separable with two irreducible quadratic factors } g_1 \text{ and } g_2 \text{ with roots } \alpha_1, \alpha_2, \alpha_3, \text{ and } \alpha_4 \text{ satisfying } \alpha_1\alpha_2 = \alpha_3\alpha_4 \},$$

$$E_4(d) = \{ f \in f_q[t] \mid \partial f = d,\ f \text{ is separable with an irreducible quadratic factor } g_1 \text{ and two linear factors } h_1 \text{ and } h_2 \text{ with roots } \alpha_1, \alpha_2, \alpha_3, \text{ and } \alpha_4 \text{ satisfying } \alpha_1\alpha_2 = \alpha_3\alpha_4 \}.$$

It is quickly seen that the probability of f belonging to two of these sets simultaneously is $O(q^{-2})$. This completes the proof of Theorem 21. Theorem 2 follows immediately from this together with Lemma 14. □

4. Exterior squares of matrices

In this section, we shall prove Theorem 3. We shall prove the third bound of Theorem 3 in Lemma 23, the first bound in Theorem 29 and finally the second bound after Theorem 30. We begin by proving

Lemma 22. *For $d \geqslant 3$, the probability that $X \in \mathrm{GL}(d,q)$ is non-semisimple is $q^{-1} + O(q^{-2})$.*

Proof. From [6, Theorem 3.1], we have

$$\mathrm{Prob}\big[X \in \mathrm{GL}(d,q) \text{ is non-cyclic}\big] = O\big(q^{-3}\big). \tag{20}$$

It follows from [7, Eq. (6.20)] that

$$\mathrm{Prob}\big[X \in \mathrm{GL}(d,q) \text{ is separable}\big] = 1 - q^{-1} + O\big(q^{-2}\big). \tag{21}$$

The result now follows by noting that

$$\begin{aligned} \mathrm{Prob}\big[X \in \mathrm{GL}(d,q) \text{ is separable}\big] &\leqslant \mathrm{Prob}\big[X \in \mathrm{GL}(d,q) \text{ is semisimple}\big] \\ &\leqslant \mathrm{Prob}\big[X \in \mathrm{GL}(d,q) \text{ is separable or non-cyclic}\big]. \end{aligned} \tag{22}$$

and substituting from (20) and (21) into (22). □

The following lemma gives us the third bound in Theorem 3.

Lemma 23. *For $d \geqslant 3$, $P_{\mathrm{nss}}(d,q) = q^{-1} + O(q^{-2})$.*

Proof. This follows from Lemma 22 and the fact shown in Theorem 13 that, for $d \geqslant 3$, X is semisimple if and only if $X^{\wedge 2}$ is semisimple. □

Recall that polynomial $f \in \mathbb{F}_q[t]$ is nearly separable if $f(t) = (t-\lambda)^2 g(t)$ where g is separable and $g(\lambda) \neq 0$. Define a matrix $X \in \mathrm{GL}(d,q)$ to be nearly separable if c_X is nearly separable.

Theorem 24. *Let p be the proportion of matrices in $\mathrm{GL}(d,q)$ that are neither separable nor both nearly separable and cyclic. Then*

$$p < 2q^{-2} + \frac{8}{9}q^{-3}.$$

The proof of Theorem 24 will follow from three lemmas. We will give the proof for the first. The proofs of the others are similar.

Lemma 25. *Let p_1 denote the probability that a matrix chosen at random from $\mathrm{GL}(d,q)$ is cyclic and has characteristic polynomial having an irreducible factor f of multiplicity at least three. Then*

$$p_1 < q^{-2} + \frac{11}{18}q^{-4}.$$

Proof. Let $V := \mathbb{F}_q^d$ and let $r := \partial f$. Having fixed r, the number of choices for f is bounded above by $(q^r - 1)/r$. Let $|\mathrm{Stab}(3r, V)|$ denote the size of the stabiliser of a $3r$-dimensional subspace of V under the action of $\mathrm{GL}(V)$. Then the number of choices for a $3r$-dimensional subspace U of V is equal to $|\mathrm{GL}(V)|/|\mathrm{Stab}(3r, V)|$. With an appropriate ordering of our basis for V, any linear map in the stabiliser of U will have corresponding matrix of the form

$$S = \begin{pmatrix} A & 0 \\ B & C \end{pmatrix}$$

where A is invertible of size $3r$, C is invertible of size $d - 3r$, and B is an arbitrary $(d-3r) \times 3r$ matrix. Counting the number of choices for A, B, and C then gives the size of the stabiliser of U, that is, $|\mathrm{Stab}(3r, V)|$ to be $|\mathrm{GL}(U)||\mathrm{GL}(V/U)|q^{3r(d-3r)}$. Hence the number of choices for U is

$$\frac{|\mathrm{GL}(V)|}{|\mathrm{GL}(U)||\mathrm{GL}(V/U)|q^{3r(d-3r)}}.$$

Next we choose α_0, an element of $\mathrm{GL}(U)$ with $\mathrm{c}_{\alpha_0}(t) = \mathrm{m}_{\alpha_0}(t) = (f(t))^3$. This is equivalent to choosing a matrix X_0 conjugate to $C(f^3)$ in $\mathrm{GL}(3r,q)$ so the number of choices is $|\mathrm{GL}(U)|/|\mathrm{Cent}(C(f^3))|$ and this is equal to $|\mathrm{GL}(U)|/((q^r-1)q^{2r})$. We now extend X_0 to a matrix X in $\mathrm{GL}(d,q)$. This can be done in $|\mathrm{GL}(V/U)|q^{3r(d-3r)}$ ways since X will have the form

$$X = \begin{pmatrix} X_0 & 0 \\ B & C \end{pmatrix}$$

where B is an arbitrary $(d-3r)\times 3r$ matrix and C is invertible of size $d-3r$, the dimension of V/U.

Hence we find that, for given r, the number of choices for X is bounded above by $|\mathrm{GL}(V)|/(rq^{2r})$. Therefore, the total number of cyclic matrices in $\mathrm{GL}(V)$ whose characteristic polynomial has an irreducible factor of multiplicity at least three is bounded above by

$$\sum_{r=1}^{d}\frac{|\mathrm{GL}(V)|}{rq^{2r}}.$$

It follows that

$$p_1 \leqslant \sum_{r=1}^{d}\frac{1}{rq^{2r}},$$

which is bounded above by

$$\frac{1}{q^2}+\frac{1}{2q^4}+\frac{1}{3}\left(\frac{1}{q^6}+\frac{1}{q^8}+\frac{1}{q^{10}}+\cdots\right)<\frac{1}{q^2}+\frac{11}{18q^4}. \qquad \square$$

Lemma 26. *Let p_2 be the probability that a matrix chosen at random from $\mathrm{GL}(d,q)$ is cyclic and has characteristic polynomial having one repeated irreducible factor of degree at least two. Then*

$$p_2<\frac{1}{2}q^{-2}+\frac{7}{12}q^{-3}.$$

Lemma 27. *Let p_3 be the probability that a matrix chosen at random from $\mathrm{GL}(d,q)$ is cyclic and has characteristic polynomial having two linear factors of multiplicity at least two. Then*

$$p_3<\frac{1}{2}q^{-2}.$$

Proof of Theorem 24. The proof follows from the fact that the sum of p_1, p_2, and p_3 forms a strict upper bound for p. $\square$

We will denote by $[z^i]g(z)$ the coefficient of z^i in the Maclaurin expansion of $g(z)$.

Lemma 28. *Let g_1 be a fixed monic irreducible quartic in $\mathbb{F}_q[t]$. Let g_2 and g_3 be a fixed pair of distinct monic irreducible quadratics in $\mathbb{F}_q[t]$. Let $\lambda_1,\lambda_2,\lambda_3$, and λ_4 be fixed distinct non-zero elements of $\mathbb{F}_q$. Let $p_k(d,q)$ be the probability that $X\in\mathrm{GL}(d,q)$ is separable and satisfies condition (k) below*:

(1) $c_X(1) \neq 0$, (2) $c_X(\lambda_j) \neq 0$ *for* $1 \leqslant j \leqslant 4$,

(3) $g_1 \nmid c_X$, (4) $g_2, g_3 \nmid c_X$,

(5) $g_2 \nmid c_X$ *and* $c_X(\lambda_1), c_X(\lambda_2) \neq 0$.

Then modulo $O(q^{-2})$ *and for* $d \geqslant 2$, $p_1(d,q) = 1 - 2q^{-1}$, $p_2(d,q) = 1 - 5q^{-1}$, $p_3(d,q) = p_4(d,q) = 1-q^{-1}$, *and* $p_5(d,q) = 1-3q^{-1}$. *Again working modulo* $O(q^{-2})$, *we have that* $p_1(1,q) = 1-q^{-1}$, $p_2(1,q) = 1-4q^{-1}$, $p_3(1,q) = p_4(1,q) = 1-q^{-1}$, *and* $p_5(1,q) = 1-2q^{-1}$.

Proof. We begin by considering $p_2(d,q)$. Fix n distinct monic irreducible polynomials $f_1, \ldots, f_n$. Then, invoking Corollary 2.3 from [5], the number of matrices conjugate to

$$A = \bigoplus_{i=1}^{n} C(f_i)$$

is

$$\frac{|\mathrm{GL}(d,q)|}{|\mathrm{Cent}(A)|} = \frac{|\mathrm{GL}(d,q)|}{\prod_{i=1}^{n}(q^{\deg f_i}-1)}.$$

It follows that the probability of a matrix $X \in \mathrm{GL}(d,q)$ being separable equals

$$\big[z^d\big] \prod_{f \in I^+} \left(1 + \frac{z^{\deg f}}{q^{\deg f}-1}\right)$$

where I^+ is the set of irreducible polynomials in $\mathbb{F}_q[t]$ excepting t. This result is well known (see, for example, [2]). From Wall [7], we have that

$$\mathrm{Prob}\big[X \in \mathrm{GL}(d,q) \text{ is separable}\big] = 1 - q^{-1} + v(q)$$

where

$$-\frac{243}{16}q^{-2} \leqslant v(q) \leqslant \frac{243}{16}q^{-2}.$$

(We use $k = 1$ and $c = 3/2$ in [7, (6.21)].) Hence

$$\prod_{f \in I^+} \left(1 + \frac{z^{\deg f}}{q^{\deg f}-1}\right) = 1 + z + \big(1 - q^{-1} + v(q)\big) \sum_{i=2}^{\infty} z^i.$$

The probability that X is separable but $c_X(\lambda_j) \neq 0$ for $1 \leqslant j \leqslant 4$ is the coefficient of z^d in

$$\left(1+\frac{z}{q-1}\right)^{-4}\prod_{f\in I^+}\left(1+\frac{z^{\deg f}}{q^{\deg f}-1}\right)$$
$$=\left(1+\frac{z}{q-1}\right)^{-4}\left(1+z+\left(1-q^{-1}+v(q)\right)\sum_{i=2}^{\infty}z^i\right).$$

For $d\geqslant 2$, it is quickly seen that this is $1-5q^{-1}+O(q^{-2})$. It is clear that $p_2(1,q)=1-4q^{-1}-O(q^{-2})$. The result for $p_1(d,q)$ is proved similarly.

To find $p_5(d,q)$, we note that the constant and q^{-1} term in

$$\left[z^d\right]\left(1+\frac{z}{q-1}\right)^{-2}\left(1+\frac{z^2}{(q^2-1)}\right)^{-1}\left(1+z+\left(1-q^{-1}+v(q)\right)\sum_{i=2}^{\infty}z^i\right)$$

is the same as that in

$$\left[z^d\right]\left(1+\frac{z}{q-1}\right)^{-2}\left(1+z+\left(1-q^{-1}+v(q)\right)\sum_{i=2}^{\infty}z^i\right).$$

It is then quickly seen that $p_5(d,q)=1-2q^{-1}+O(q^{-2})$. The proofs for $p_3(d,q)$ and $p_4(d,q)$ are similar. □

In what follows, we denote the set of all monic separable polynomials of degree n in $\mathbb{F}_q[t]$ by $\sigma(n)$. Given a monic polynomial f in $\mathbb{F}_q[t]$, we denote the number of distinct irreducible factors it has by s_f and denote the degrees of its distinct irreducible factors by $d_{1,f},d_{2,f},\ldots,d_{s_f,f}$. The next theorem proves the first bound of Theorem 3.

Theorem 29. $P_{\mathrm{ns}}(d,q)=2q^{-1}+O(q^{-2})$.

Proof. Recall the sets $E_1(d),\ldots,E_4(d)$ defined in Section 2. Also define

$$E_5(d)=\left\{f\in\mathbb{F}_q[t]\;\middle|\;\begin{array}{l}f \text{ is monic and separable with an irreducible cubic factor } g_1 \text{ with}\\ \text{roots } \alpha_1,\alpha_2, \text{ and } \alpha_3 \text{ and an irreducible quadratic or linear factor } g_2\\ \text{with root } \alpha_4 \text{ such that } \alpha_1\alpha_2=\alpha_3\alpha_4\end{array}\right\}.$$

Define

$$E(d)=\bigcup_{1\leqslant i\leqslant 5}E_i(d).$$

Recall from the proof of Theorem 21 that we split separable polynomials f with non-separable exterior squares into five cases. For $1\leqslant i\leqslant 5$, let $A_i(d)$ denote the set of polynomials of degree d in case i. For $1\leqslant i\leqslant 5$, define $B_i(d)=A_i(d)\setminus E(d)$. Finally, define

$$A_6(d):=\left\{f\in\mathbb{F}_q[t]\;\middle|\; f \text{ of degree } d \text{ is monic and nearly separable}\right\}.$$

From Theorem 24, the proportion of matrices $X \in \mathrm{GL}(d,q)$ which are neither separable nor both nearly separable and cyclic is less than $\frac{22}{9}q^{-2}$. So, if we define

$$A(d) = \bigcup_{1 \leqslant i \leqslant 6} A_i(d),$$

we have

$$P_{\mathrm{ns}}(d,q) = \sum_{f \in A(d)} \mathrm{Prob}\big[X \text{ is cyclic and has } \mathrm{c}_X(t) = f(t)\big] + O\big(q^{-2}\big). \tag{23}$$

Define

$$B(d) = \bigcup_{1 \leqslant i \leqslant 5} B_i(d).$$

Then we have that

$$A(d) = A_6(d) \,\dot\cup\, B(d) \,\dot\cup\, E(d).$$

Let us begin by finding

$$\sum_{f \in A_6(d)} \mathrm{Prob}\big[X \in \mathrm{GL}(d,q) \text{ is cyclic with } \mathrm{c}_X = f\big].$$

Firstly, we choose $\lambda \in \mathbb{F}_q^*$. Invoking Corollary 2.3 of [5], we find that the number of matrices in $\mathrm{GL}(d,q)$ which are cyclic and nearly separable with characteristic polynomial $(t-\lambda)^2 f(t)$ for some f is

$$\sum_{f \in S_\lambda} \frac{|\mathrm{GL}(d,q)|}{q^d(1-q^{-1})\prod_{i=1}^{s_f}(1-q^{-d_{i,f}})}$$

where S_λ is the set of monic separable polynomials in $\mathbb{F}_q[t]$ of degree $d-2$ which do not have λ as a root. There are $q-1$ choices for λ. Hence

$$\begin{aligned}
&\mathrm{Prob}\big[X \in \mathrm{GL}(d,q) \text{ is cyclic and nearly separable}\big] \\
&= \sum_{\lambda \in \mathbb{F}_q^*} \sum_{f \in S_\lambda} \frac{1}{q^d(1-q^{-1})\prod_{i=1}^{s_f}(1-q^{-d_{i,f}})} \\
&= \frac{(q-1)}{q^2(1-q^{-1})} \sum_{f \in S_1} \frac{1}{q^{d-2}\prod_{i=1}^{s_f}(1-q^{-d_{i,f}})} \\
&= q^{-1} \times \mathrm{Prob}\big[X \in \mathrm{GL}(d-2,q) \text{ is separable and } \mathrm{c}_X(1) \neq 0\big] \\
&= q^{-1} + O\big(q^{-2}\big),
\end{aligned}$$

using Lemma 28.

Now we will show that

$$\sum_{f\in B(d)} \text{Prob}\big[X \text{ is cyclic and has } c_X(t) = f(t)\big] = O\big(q^{-2}\big). \tag{24}$$

Firstly, note that this sum is bounded above by

$$\sum_{1\leqslant i\leqslant 5} \sum_{f\in B_i(d)} \text{Prob}\big[X \text{ is cyclic and has } c_X(t) = f(t)\big].$$

We will show that

$$\sum_{f\in B_i(d)} \text{Prob}\big[X \text{ is cyclic and has } c_X(t) = f(t)\big] = O\big(q^{-2}\big)$$

for $i = 1$ and 3. The proofs for $B_2(d), B_4(d), B_5(d)$ are similar. We begin by defining $C(n)$ to be the set of monic irreducible polynomials of degree n which have a root α such that $\alpha^{1+q^i} = \alpha^{q^j+q^k}$ for some i, j, k. From the index cycling argument, we know that $|C(n)| \leqslant q^{\lfloor 3n/4\rfloor}$. Note that

$$\begin{aligned}
&\sum_{f\in B_1(d)} \text{Prob}\big[X \text{ is cyclic and has } c_X(t) = f(t)\big] \\
&< \sum_{n=5}^{\infty} \sum_{g\in C(n)} \frac{1}{q^n(1-q^{-n})} \sum_{h\in\sigma(d-n)} \frac{1}{q^{d-n}\prod_{i=1}^{s_h}(1-q^{-d_{i,h}})} \\
&< \sum_{n=5}^{\infty} \frac{q^{-\lceil n/4\rceil}}{(1-2^{-5})} \sum_{h\in\sigma(d-n)} \frac{1}{q^{d-n}\prod_{i=1}^{s_h}(1-q^{-d_{i,h}})} \\
&= \sum_{n=5}^{\infty} \frac{q^{-\lceil n/4\rceil}}{(1-2^{-5})} \text{Prob}\big[X \in \mathrm{GL}(d-n,q) \text{ is separable}\big] \\
&= O\big(q^{-2}\big) \times \big(1 - q^{-1} + O\big(q^{-2}\big)\big) = O\big(q^{-2}\big).
\end{aligned}$$

Now define $C(n_1, n_2)$ to be the set of pairs g_1, g_2 of monic irreducible polynomials of degrees n_1 and n_2, respectively, with roots α_1 and α_2, respectively, such that $\alpha_1^{1+q^i} = \alpha_2^{1+q^j}$ for some i and j. We may assume without loss of generality that $n_1 \geqslant n_2$. From an index cycling argument we have that $|C(n_1, n_2)| \leqslant q^{n_2+\lfloor n_1/2\rfloor}$. Let

$$R(q) = \frac{1}{q^{n_1+n_2}(1-q^{-n_1})(1-q^{-n_2})}.$$

Then

$$\begin{aligned}
&\sum_{f\in B_3(d)} \operatorname{Prob}\big[X \text{ is cyclic and has } \mathrm{c}_X(t) = f(t)\big] \\
&< \sum_{n_1=3}^{\infty}\sum_{n_2=2}^{n_1}\sum_{C(n_1,n_2)} R(q) \sum_{h\in\sigma(d-n_1-n_2)} \frac{1}{q^{d-n_1-n_2}\prod_{i=1}^{s_h}(1-q^{d_{i,h}})} \\
&= \sum_{n_1=3}^{\infty}\sum_{n_2=2}^{n_1}\sum_{C(n_1,n_2)} R(q)\operatorname{Prob}\big[X \in \mathrm{GL}(d-n_1-n_2,q) \text{ is separable}\big] \\
&= \sum_{n_1=3}^{\infty}\sum_{n_2=2}^{n_1}\sum_{C(n_1,n_2)} R(q)\big(1-q^{-1}+O\big(q^{-2}\big)\big) \\
&< \big(1-q^{-1}+O\big(q^{-2}\big)\big)\sum_{n_1=3}^{\infty}\frac{n_1 q^{-\lceil n_1/2\rceil}}{(1-2^{-2})(1-2^{-3})} = O\big(q^{-2}\big).
\end{aligned}$$

Now we turn to $E(d)$. To find

$$\sum_{f\in E_1(d)} \operatorname{Prob}\big[X \in \mathrm{GL}(d,q) \text{ is cyclic with } \mathrm{c}_X = f\big],$$

we choose an irreducible quartic g such that $g^{\wedge 2}$ is non-separable. The number of matrices in $\mathrm{GL}(d,q)$ which are separable with $\mathrm{c}_X(t) = g(t)f(t)$ for some f, is

$$\sum_{f\in S_g} \frac{|\mathrm{GL}(d,q)|}{q^d(1-q^{-4})\prod_{i=1}^{f_s}(1-q^{-d_{i,f}})}$$

where S_g is the set of monic separable polynomials of degree $d-4$ in $\mathbb{F}_q[t]$ which do not have g as a factor. Let Q_4 be the set of monic irreducible quartics which have a non-separable exterior square. Then

$$\operatorname{Prob}\big[X \in \mathrm{GL}(d,q) \text{ has } \mathrm{c}_X \in E_1(d)\big] \leqslant P$$

where

$$P = \sum_{g\in Q_4}\sum_{f\in S_g} \frac{1}{q^d(1-q^{-4})\prod_{i=1}^{s_f}(1-q^{-d_{i,f}})}.$$

From Section 2, we know that $|Q_4| = \frac{1}{4}q^3 + O(q^2)$. Hence

$$P = \frac{\big(\frac{1}{4}q^3+O(q^2)\big)}{q^4(1-q^{-4})}\sum_{f\in S_g}\frac{1}{q^{d-4}\prod_{i=1}^{s_f}(1-q^{-d_{i,f}})}$$

$$= \left(\frac{1}{4}q^{-1} + O\left(q^{-2}\right)\right) \times \text{Prob}\left[X \in \text{GL}(d-4,q) \text{ is separable with } g_1 \nmid c_X\right]$$

where g_1 is a fixed irreducible quartic in $\mathbb{F}_q[t]$. Invoking Lemma 28, we see that this equals $\frac{1}{4}q^{-1} + O(q^{-2})$.

Now note that

$$\text{Prob}\left[X \in \text{GL}(d,q) \text{ has } c_X \in E_1(d)\right] \geqslant P - \sum_{g_1,g_2} \sum_{S_{g_1,g_2}} \frac{1}{q^d(1-q^{-4})^2 \prod_{i=1}^{s_f}(1-q^{-d_{i,f}})},$$

where S_{g_1,g_2} is the set of monic separable polynomials of degree $d-8$ in $\mathbb{F}_q[t]$ which do not have g_1 or g_2 as a factor, and the outer sum is over all (unordered) pairs g_1, g_2 of distinct irreducible quartics which have a non-separable exterior square. However,

$$\begin{aligned}
&\sum_{g_1,g_2} \sum_{S_{g_1,g_2}} \frac{1}{q^d(1-q^{-4})^2 \prod_{i=1}^{s_f}(1-q^{-d_{i,f}})} \\
&\quad \leqslant \frac{|N_4|^2}{q^8(1-q^{-4})^2} \sum_{S_{g_1,g_2}} \frac{1}{q^{d-8} \prod_{i=1}^{s_f}(1-q^{-d_{i,f}})} \\
&\quad = \frac{|N_4|^2}{q^8(1-q^{-4})^2} \times \text{Prob}\left[X \in \text{GL}(d-4,q) \text{ is separable with } g_1, g_2 \nmid c_X\right] \\
&\quad = O\left(q^{-2}\right) \times \left(1 - q^{-1} + O\left(q^{-2}\right)\right) = O\left(q^{-2}\right).
\end{aligned}$$

Hence

$$\text{Prob}\left[X \in \text{GL}(d,q) \text{ has } c_X \in E_1(d)\right] = \frac{1}{4}q^{-1} + O\left(q^{-2}\right). \tag{25}$$

From Section 2, we know that the proportions of monic polynomials of degree d in the sets $E_2(d)$, $E_3(d)$, $E_4(d)$, and $E_5(d)$ are respectively $\frac{3}{8}q^{-1}$, $\frac{1}{8}q^{-1}$, $\frac{1}{4}q^{-1}$, and 0 modulo $O(q^{-2})$. Using this fact and the same method used to find Prob[$X \in \text{GL}(d,q)$ has $c_X \in E_1(d)$] we find that Prob[$X \in \text{GL}(d,q)$ has $c_X \in E_i(d)$] equals $\frac{1}{8}q^{-1}$, $\frac{3}{8}q^{-1}$, $\frac{1}{4}q^{-1}$, and 0 modulo $O(q^{-2})$ for $i = 2, 3, 4$, and 5, respectively.

Also from Section 2, we know that the proportion of monic polynomials of degree d in the sets $E_i(d) \cap E_j(d)$ for $1 \leqslant i < j \leqslant 5$ is $O(q^{-2})$. Using this fact and a similar method to that used above, we find that

$$\text{Prob}\left[X \in \text{GL}(d,q) \text{ has } c_X \in E_i(d) \cap E_j(d)\right] = O\left(q^{-2}\right)$$

for $1 \leqslant i < j \leqslant 5$. The result now follows. □

We now move on to look at the probability that a matrix $X \in \text{GL}(d,q)$ has a non-cyclic exterior square. Using Theorem 24 we have that, modulo $O(q^{-2})$, $P_{\text{nc}}(d,q)$ equals the

probability that $X \in \mathrm{GL}(d,q)$ is separable or both nearly separable and cyclic and has a non-cyclic exterior square. We will now show that

$$\mathrm{Prob}\big[X \in \mathrm{GL}(d,q) \text{ is nearly separable and cyclic with } X^{\wedge 2} \text{ non-cyclic}\big] = O\big(q^{-2}\big).$$

It will follow that

$$P_{\mathrm{nc}}(d,q) = \mathrm{Prob}\big[X \in \mathrm{GL}(d,q) \text{ is separable and has } X^{\wedge 2} \text{ non-cyclic}\big] + O\big(q^{-2}\big). \quad (26)$$

Theorem 30. *The probability that $X \in \mathrm{GL}(d,q)$ is cyclic with a nearly separable characteristic polynomial but has a non-cyclic exterior square is $O(q^{-2})$.*

Proof. Let g be a separable polynomial of degree $d-2$ with non-zero constant term and let $C(g)$ denote the companion matrix of g. Let the roots of g in its splitting field be α_i for $1 \leqslant i \leqslant d-2$. Suppose that

$$X = C(g) \oplus \begin{pmatrix} \lambda & 1 \\ 0 & \lambda \end{pmatrix}.$$

Then $X^{\wedge 2} = C(g^{\wedge 2}) \oplus (\lambda^2) \oplus B$ where

$$B = \bigoplus_{1 \leqslant i \leqslant d-2} \begin{pmatrix} \lambda\alpha_i & \alpha_i \\ 0 & \lambda\alpha_i \end{pmatrix}. \quad (27)$$

Since the summands in (27) are cyclic with coprime minimal polynomials, we have that B is cyclic. Hence $X^{\wedge 2}$ is non-cyclic if and only if either

$$\alpha_i\alpha_j = \alpha_k\alpha_l \quad \text{or} \quad \lambda^2 = \alpha_i\alpha_j \quad \text{or} \quad \lambda\alpha_i = \alpha_j\alpha_k$$

for some i, j, k, l.

We consider the following cases separately.

Case 1: $\alpha_i\alpha_j = \alpha_k\alpha_l$.
Case 2: $\lambda^2 = \alpha_i\alpha_j$. This splits into the cases where α_i and α_j belong to distinct irreducible factors of g and where they do not.
Case 3: $\lambda\alpha_i = \alpha_j\alpha_k$. This splits into three cases, depending on whether exactly one, two or three of the roots α_l belong to the same irreducible factor of g.

Here we will give the argument used to deal with Cases 1 and 2A where both roots belong to the same irreducible factor of g. The others are similar.

Case 1 ($\alpha_i\alpha_j = \alpha_k\alpha_l$). Let

$$A(d) := \big\{ g \in \mathbb{F}_q[t] \;\big|\; g \text{ is separable, has degree } d-2 \text{ and has roots } \alpha_1, \alpha_2, \alpha_3, \text{ and } \alpha_4 \text{ such that } \alpha_1\alpha_2 = \alpha_3\alpha_4 \big\}.$$

Let $\pi_1(d,q)$ be the probability that $X \in \mathrm{GL}(d,q)$ is conjugate to $C(g) \oplus C((t-\lambda)^2)$ for some $\lambda \in \mathbb{F}_q^*$ and for some $g \in A(d)$ such that $g(\lambda) \neq 0$. Then

$$\begin{aligned}\pi_1(d,q) &\leqslant \sum_{\lambda\in\mathbb{F}_q^*}\sum_{g\in A(d)} \frac{1}{(q^2-q)q^{d-2}\prod_{i=1}^{s_g}(1-q^{-d_{i,g}})}\\ &= \sum_{\lambda\in\mathbb{F}_q^*}\frac{1}{(q^2-q)}\sum_{g\in A(d)}\frac{1}{q^{d-2}\prod_{i=1}^{s_g}(1-q^{-d_{i,g}})}\\ &= q^{-1}\,\mathrm{Prob}\big[X \in \mathrm{GL}(d-2,q) \text{ is separable and has } X^{\wedge 2} \text{ non-separable}\big]\\ &\leqslant q^{-1}\big(2q^{-1}+O\big(q^{-2}\big)\big) = O\big(q^{-2}\big),\end{aligned}$$

using Theorem 29.

Case 2A. Let $\alpha := \alpha_i$ and let n be the degree of the minimum polynomial of α. It follows that n is even and $\lambda^2 = \alpha^{1+q^{n/2}}$. Define $A_\lambda(n)$ to be the set

$$\big\{h \in \mathbb{F}_q[t] \;\big|\; \partial h = n,\ h \text{ is monic irreducible with root } \alpha \text{ such that } \alpha^{1+q^{n/2}} = \lambda^2\big\}.$$

Then it is clear that $|A_\lambda(n)| \leqslant Kq^{n/2}$ for some constant K.

Define $\pi_{2A}(d,q)$ to be the probability the probability that $X \in \mathrm{GL}(d,q)$ is conjugate to $C(g) \oplus C((t-\lambda)^2)$ for some $\lambda \in \mathbb{F}_q$ and some separable $g = hh_1$ such that $h_1 \in A_\lambda(n)$ and $\deg h = d-2-n$. Then

$$\pi_{2A}(d,q) \leqslant \sum_{\lambda\in\mathbb{F}_q^*}\sum_{n\ \text{even}}\sum_{h_1\in A_\lambda(n)}\sum_{h}\frac{1}{q^2(1-q^{-1})}\frac{1}{q^n(1-q^{-n})}\frac{1}{q^{d-2-n}\prod_{i=1}^{s_h}(1-q^{-d_{h,i}})}$$

where the innermost sum is over all separable $h \in \mathbb{F}_q[t]$ of degree $d-2-n$. This upper bound is at most

$$\begin{aligned}&\sum_{\lambda\in\mathbb{F}_q^*}\frac{1}{q^2(1-q^{-1})}\sum_{n\ \text{even}}\frac{Kq^{n/2}}{q^n(1-q^{-n})}\sum_{h}\frac{1}{q^{d-2-n}\prod_{i=1}^{s_h}(1-q^{-d_{i,h}})}\\ &\leqslant Kq^{-1}\sum_{n\ \text{even}}\frac{q^{-n/2}}{(1-2^{-1})}\sum_{h}\frac{1}{q^{d-2-n}\prod_{i=1}^{s_h}(1-q^{-d_{i,h}})}\\ &\leqslant Kq^{-1}\sum_{n\ \text{even}}2q^{-n/2}\,\mathrm{Prob}\big[X \in \mathrm{GL}(d-2-n,q) \text{ is separable}\big] = O\big(q^{-2}\big).\end{aligned}$$

This completes the proof of Theorem 30. □

As we commented earlier at (26), it now follows that

$$P_{\mathrm{nc}}(d,q) = \mathrm{Prob}\big[X \in \mathrm{GL}(d,q) \text{ is separable and has } X^{\wedge 2} \text{ non-cyclic}\big] + O\big(q^{-2}\big). \quad (28)$$

If X is separable then X is semisimple which implies that $X^{\wedge 2}$ is semisimple (see Section 2). Hence for X separable, $X^{\wedge 2}$ is non-cyclic if and only if $X^{\wedge 2}$ is non-separable. Therefore, (28) becomes

$$\begin{aligned} P_{\mathrm{nc}}(d,q) &= \mathrm{Prob}\big[X \in \mathrm{GL}(d,q) \text{ is separable and has } X^{\wedge 2} \text{ non-separable}\big] + O\big(q^{-2}\big) \\ &= q^{-1} + O\big(q^{-2}\big), \end{aligned}$$

as was shown in the proof of Theorem 29. This gives us the second bound of Theorem 3 and hence completes its proof.

Acknowledgments

The work in this paper is taken from the author's DPhil thesis. The author records his warm thanks to his supervisor Dr Peter Neumann and extends his gratitude to the Carnegie Trust for funding this research.

References

[1] D. Brydon, Exterior squares over finite fields: polynomials, matrices and probabilities, DPhil thesis, University of Oxford, 2001.
[2] J. Fulman, Cycle indices for the finite classical groups, J. Group Theory 2 (1999) 251–289.
[3] C. Greenhill, An algorithm for recognising the exterior square of a matrix, Linear and Multilinear Algebra 46 (1999) 213–244.
[4] C. Greenhill, An algorithm for recognising the exterior square of a multiset, DPhil thesis. University of Oxford, 1999.
[5] P.M. Neumann, C.E. Praeger, Cyclic matrices over finite fields, J. London Math. Soc. (2) 52 (1995) 263–284.
[6] P.M. Neumann, C.E. Praeger, Cyclic matrices in classical groups over finite fields, J. Algebra 234 (2000) 367–418.
[7] G.E. Wall, Counting cyclic and separable matrices over a finite field, Bull. Austral. Math. Soc. 60 (1999) 253–284.